Cyber Security in the Era of Digital Transformation

Jiří Kaplický

June 2016
Agenda

• Digital Transformation in the Cyber Security context
• Shift from analog word to fully digital - Is everybody prepared?
• Go digital, reduce fraud!
• Technology trends and new authentication methods
• Identity Management in Transition - from Employees to Customers
Cyber Security in the Era of Digital Transformation

- Digital Transformation
  - Acceleration of business activities, processes, competencies and models
  - New business models, new technologies, new …
  - New opportunities for cyber criminals
- Cyber Security = pillar of Digital transformation

Cyber Security is no more an IT issue – it’s a business issue
From analog to digital – is everybody prepared?

- Is everybody prepared for NEW ….
- New technologies and processes may be hip, but also complicated

VS
Paperless

- Transition from analog documents to digital
  - Signature, validation, archiving
- eIDAS – end of uncertainty in Identity EU region
  - Enabler of European Digital Single Market
Biometry - Dynamic Signature
New technology as transition enabler

Dynamic signature is a biometric modality that uses, for recognition purposes, the anatomic and behavioral characteristics that an individual exhibits when signing his or her name (or other phrase).

- New technology still uses well known method – handwritten signature
- Captured image is enriched with:
  - direction, stroke, pressure …
- Legally recognized – fulfills most req. the Act No. 227/2000 Coll.

More than 50 primary and 600 secondary characteristics are extracted, weighed and compared using a neural network and fuzzy

Dynamic Signals

Start and end of strokes

pressure

speed

Pressure Levels

time

Enclosed Areas

Curves and Loops

Crossings

Upstrokes

S. Schmitt

S. Schmitt

S. Schmitt

S. Schmitt
eIDAS Directive
Accelerator of Digital Transformation

- Central role of eID
- Cross border
  - Interoperability
  - Harmonization
- Key processes
  - Sign
  - Validate
  - Archive
Digital Transformation and Fraud

• The Digital Single Market: Trust and security as key drivers
  • Trust in digital is critical for customers
  • Security as the top priority

Internet users express concern about being the victim of bank card or online banking fraud (63%) and fear their social media or email account being hacked (60%)

February 2015 Eurobarometer survey on Cyber-security

Protect the bank
Financial crime is costly and complex

Key challenges for FS Companies

The financial crime landscape
- Ever more complex and sophisticated
- Regulators are not synchronized
- Transaction volumes are growing

The traditional approach is flawed
- Fraudsters continue to bypass and evade the banks’ controls
- Silos of applications don’t drive the efficiencies required

The costs are also growing
- Fines are increasing
- Complex to implement on legacy
- Reputation damage impacts share price, profits and RoE
CGI’s “protect the bank”

...delivered through the combination and investment of CGI IP
CENTAUR Overview:

- Monitors account behavior across single and multiple channels using internal and external data
- Pre-defined rules to detect suspicious (client or employee) activities and transactions
- Ability to recommend modifications to the model
- High-performance scalable real-time risk engine
- Big Data Analytics Platform

BENEFITS:

- High speed and real time
  - Enables use on new instruments – eg. Immediate Payments
- Flexible design enables rapid implementation and integration of Cyber, Case Management etc.
- Can be utilized as a stand alone solution
- Transparent “open” approach
IAM in Digital Transformation Era

• Key challenges of IAM
  • IAM re-aligned with today’s digital and cyber eco-system
  • Identity Federation
  • Open APIs
  • Demand for authentication methods resilient to fraud
  • IAM in Transition - from Employees to Customers

• New trends and methods
  • Context / risk based – geolocation, device, operation, time
  • Biometrics
    • Vein, iris, fingerprints, voice …
    • Commercial solutions - Apple TouchID, Android M (6.0), Windows Hello, CGI éligo
  • Behavioral
    • Keystroke, cursor movements
Rethink IAM

Current state of IAM

Future state of IAM
Future IAM and API requirements

• Identity Broker
  • Federated identity
  • Support for multiple authentication methods
  • Multiprotocol support – SAML, JWS, Oauth

• Openness of the Digital Economy requires Open APIs
• Security Requirements for Open APIs
  • Unified solution for API protection and audit – API GW
  • Different clients – different requirements
    • Data sets
    • Protocols
    • Authentication methods
    • Authorization schemes
Our commitment to you
We approach every engagement with one objective in mind: to help clients succeed